

## REMARKS

### Objection of the Specification

The specification was objected to as allegedly failing to provide proper antecedent basis for the limitation “wherein the subsequent transmissions are capable of penetrating the walls of the room.” This objection is obviated by the present amendments. For example, claim 21 was amended to specifically state that conference data transmissions are capable of penetrating the walls of the room. The specification provides antecedent basis and support for conference data transmission can be transmitted using RF signals. See, e.g., paragraph [0011] (“The encryption key is subsequently utilized by the base station and remote devices to encrypt and decrypt conference data passed between and among the devices and the base station through RF signals.”). The specification additionally states that RF signals can penetrate walls. See, e.g., paragraph [0016] (“Because RF signals transmitted by base station 106 and remote devices 108 and 110 may easily penetrate wall 104 and reach remote device 112, the information underlying the transmitted RF signals may be inadvertently disseminated to persons having access to remote device 112.”). Thus, the specification provides antecedent basis for conference data transmissions capable of penetrating walls.

### Rejections under 35 U.S.C. 112

Claims 21-29 were rejected under 35 U.S.C. 112 because the specification allegedly fails to meet the written description requirement with respect to the limitation “wherein the subsequent transmissions are capable of penetrating the walls of the room.” This rejection is obviated by the present amendment. For example, claim 21 has been amended to recite a conference data transmission that is capable of penetrating the walls of the room. As stated immediately above, this limitation is described in the specification.

Claims 21-40 were rejected under 35 U.S.C. 112 because the phrase “substantially contained” was considered indefinite. This rejection is obviated by the present amendments. For example, claim 21 has been amended to recite that the encryption key signal does not penetrate walls of the room. Support for this amendment is found at paragraph [0017], as well as throughout the specification.

### Rejections under 35 U.S.C. 103

Independent claims 21, 30, and 40 have been rejected under 35 U.S.C. 103 as being unpatentable over Schneier, in view of Parry (US 2002/0164997 A1). Essentially, the Office Action states that Schneier discloses transmitting an encryption key between a first and second device, wherein the encryption key is used to encrypt and decrypt data for subsequent transmissions between the first and second devices. The Examiner admits that Schneier fails to disclose that the transmission is wireless and that the devices are confined within a room and that the encoded encryption key is not detectable outside of the room. However, the Office Action alleges that Parry teaches the limitations not taught by Schneier.

Parry is directed to a system wherein one or more computing devices (reference numeral 12 throughout Parry) are used to define a zone and then selectively permit wireless communication access between devices 12 and additional computing devices (reference numeral 14) depending on the location of devices 14 with reference to the zone. In other words, devices 14 can talk to devices 12 only if devices 14 are within the defined zone. *See, for example, Parry abstract.*

While Parry is directed to controlling communication between devices depending on the location of the devices relative to a defined zone, Parry accomplishes this in a much different way than the presently claimed invention. The devices of Parry include a distance/location module 26, which can optionally be assisted by a global positioning satellite system 20. *See Parry, paragraph [0024].* Parry describes two methods of establishing the “zones,” which determine whether devices 12 and 14 will be allowed to communicate with each other. According to one method, each device 12 having a distance/location module 26 communicates wirelessly to identify distance/location between devices 12, thereby constructing an electronic map of the position of the devices 12. *See Parry, paragraph [0034].* The mapped positions correspond to the landmarks that establish the boundaries of the zone. *Id.* The second method described by Parry uses a global satellite positioning system to determine the absolute position of each of the devices 12 or uses an administrator to measure the boundaries of the desired pattern and enter that data into the devices 12. *See Parry, paragraph [0035].* While Parry does mention that the boundaries can of the zone can correspond to a physical boundary such as a walled room or building (paragraph [0032], cited in Office Action), there is no requirement that they do so.

More importantly, there is no teaching in Parry that the any signals transmitted by the devices of Parry are incapable of penetrating the walls.

The Office Action alleges that it would have been obvious to transmit the encoded encryption key of Schneier using the wireless transmission system of Parry. Assuming for the sake of argument that this is true, the combination of Schneier and Parry still does not teach every limitation of the rejected claims.

Each of the independent claims requires that the encryption code be transmitted by a different type of transmission than the transmission used to transmit the conference data. Specifically, the encryption code transmission is required to not penetrate walls of the room, whereas the conference data transmission signal does penetrate the walls of the room. The combination of Schneier and Parry does not teach the two types of transmissions required by the claims, i.e., the transmission of an encryption code that cannot penetrate the walls and the transmission of conference data that can penetrate the walls.

As described above Parry does not use an encryption code at all, but rather allows a remote device to access a base station only if the remote device is in a specified zone. Even if the specified zone of Parry corresponds to a room, as alleged in the Office Action, there is still no teaching in Parry of signals that cannot penetrate the walls of the room. In fact, Parry suggests that all of the transmissions can penetrate outside of the specified zone because the first computing device determines the position of the second computing device and determines whether or not the second device is within the specified zone. For example, see paragraph [0037] of Parry. In all cases, the signals of the two devices are capable of reaching each other, whether or not the second device is in the specified zone. If the second device is outside the zone, it is simply denied access to the first device. Even if access is denied, all of the signals sent between the first and second devices are capable of reaching their intended target. The technique of Parry is based on allowing or denying access based on the relative or absolute position of the requesting device, not on whether the requesting device has received the encryption code. If the second device of Parry is outside the zone, it is not denied access to the first device because it was incapable of receiving an encryption key, as in the instant claims. Rather the second device of Parry is denied access because the first device has determined that the second device is outside the zone and thus denies the second device access. As such, the combination of Schneier and Parry does not teach transmitting an encryption code such that the

transmission cannot penetrate the walls of a room but transmitting data by a transmission that can penetrate the walls.

In rejecting claims 22 and 32-35, the Office Action alleges that Parry teaches acoustic signals. However, nothing in Parry suggests using acoustic signals to transmit one type of data such as an encryption code and in same embodiment using another type of signal such as RF to transmit another type of data such as conference data. Thus, according to Parry, if the encryption code were transmitted using an acoustic signal, then the conference data would also be transmitted using an acoustic signal (incapable of penetrating walls) and the limitations of the instant independent claims would not be met.

The Office Action also alleges that Parry teaches the use of infrared communications as recited in instant claim 24. However, the infrared communications referred to in paragraph [0025] of Parry is communication between a user interface and the wireless access control system, not a signal transmitted between a first and second device, as required by the claim. If the user interface and the wireless access control system are considered as the first and second devices for the purposes of rejecting claim 24, then the rejection of independent claim 21 falls apart because in rejecting that claim the first and second devices must have been device 12 and device 14, respectively. The rejections of claims 21 and 24 are inconsistent and thus are improper.

As shown herein, the combination of Schneier and Parry fail to teach every limitation of the independent claims. The additional secondary references do not teach the missing limitation. Claims not specifically addressed in this response are patentable in view of their dependency from claims that are allowable.

\* \* \* \* \*

Based on the above, Applicant respectfully submits that the claims are patentable over the cited art and requests that a Notice of Allowance issue for these claims.

Respectfully submitted,

**January 17, 2008**

**/Raymond Reese/**  
R. Scott Reese, Reg. No. 47,891

**CUSTOMER NO. 29855**

Wong, Cabello, Lutsch,  
Rutherford & Bruculeri, L.L.P.  
20333 State Highway 249, Suite 600  
Houston, Texas 77070  
832-446-2400 (Phone)  
832-446-2424 (Fax)